Charles Lew (SBN 227495)
Charles@thelewfirm.com
Isaiah Artest (SBN 320326)
Isaiah@thelewfirm.com
THE LEW FIRM, APC
9440 Santa Monica Blvd., Suite 301
Beverly Hills, California 90210
Telephone: (310) 279-5145
Facsimile: (310) 300-1819

Damion D. D. Robinson, SBN 262573
David Markevitch, SBN 256163
Jimmie Davis Parker SBN 252023
ROBINSON MARKEVITCH & PARKER LLP
8430 Santa Monica Blvd., Suite 200
West Hollywood, California 90069
Tel. (213) 757-7778
Email: dr@robinsonmarkevitch.com
dm@robinsonmarkevitch.com
jdp@robinsonmarkevitch.com

Attorneys for Class Plaintiffs and all others similarly situated

UNITED STATES DISTRICT COURT

CENTRAL DISTRICT OF CALIFORNIA

JANE DOE 1, an individual; JANE DOE 2, an individual; JANE DOE 3, an individual; JANE DOE 4, an individual JANE DOE 5, an individual, JANE DOE 6, an individual; JANE DOE 8, an individual, JANE DOE 9, an individual; JANE DOE 10, an individual; JANE DOE 11, an individual; JANE DOE 12, an individual, JANE DOE 13, an individual, JANE DOE 14, an individual, and JANE DOE 15, an individual; JANE DOE 16, an individual; individually and on behalf of all others similarly situated

Plaintiffs,

vs.

JAIME S. SCHWARTZ, MD, an individual; JAIME S. SCHWARTZ, MD PC, a California professional corporation, KAREN L. HERBST, MD, an individual, KAREN L. HERBST, MD, PC, a California professional corporation; and TOTAL LIPEDEMA CARE, a California corporation; and DOES 1 through 10,

Case No.: 2:25-CV-00898-GW-SSC

CLASS ACTION

FIRST AMENDED COMPLAINT FOR DAMAGES, DECLARATORY, AND INJUNCTIVE RELIEF FOR:

1. **VIOLATION OF THE CONFIDENTIALITY OF MEDICAL INFORMAITON ACT;**
2. **NEGLIGENCE;**
3. **VIOLATION OF THE UNFAIR COMPETITION LAW [Cal. Bus. & Prof. Code § 17200];**
4. **INVASION OF PRIVACY; and**
5. **VIOLATION OF CALIFORNIA CIVIL CODE § 1798.80, *et seq.*;**

DEMAND FOR JURY TRIAL

inclusive,

Defendants.

Plaintiffs JANE DOE 1, an individual; JANE DOE 2, an individual; JANE DOE 3, an individual; JANE DOE 4, an individual; JANE DOE 5, an individual; JANE DOE 6, an individual; JANE DOE 8, an individual; JANE DOE 9, an individual; JANE DOE 10, an individual; JANE DOE 11, an individual; JANE DOE 12, an individual; JANE DOE 13, an individual; JANE DOE 14, an individual; JANE DOE 15, an individual; and JANE DOE 16, an individual (collectively, "Class Plaintiffs" or "Plaintiffs"), on behalf of themselves and all others similarly situated ("Class Members"), allege for their complaint against Defendants JAIME S. SCHWARTZ, MD, a California professional corporation, JAIME S. SCHWARTZ, MD PC, a California professional corporation (collectively, "Dr. Schwartz"), KAREN L. HERBST, MD, an individual; KAREN L. HERBST, MD, PC, a California professional corporation: TOTAL LIPEDEMA CARE, a California corporation; and DOES 1 through 10, inclusive (collectively with Dr. Schwartz, "Defendants") as follows. Allegations herein are made on personal knowledge as to Class Plaintiffs and information and belief as to all other matters.

INTRODUCTION

1. Dr. Schwartz is a prominent plastic surgeon with offices in Beverly Hills and Dubai. He has appeared on television networks Bravo and E! and was a featured doctor on the hit shows "Botched" and "The Doctors." On his website, Dr. Schwartz proclaims that he "respect[s]" and is "committed to protecting" patient privacy.

2. Despite charging clients thousands of dollars and having access to their deeply private medical information, Dr. Schwartz disregarded basic security measures necessary to protect that information from malicious cyberattacks. Dr. Schwartz and others in the medical field – and in the plastic surgery field specifically – have been warned for years by government agencies and professional organizations that they are

targets for hackers who seek sensitive patient data for ransom and extortion.

3. Dr. Schwartz disregarded these warnings and failed to take patient data security seriously. As a result of his negligence, he allowed his network to be compromised ***twice*** in less than a year. On information and belief, the malicious actors gained access to Dr. Schwartz entire network and all or substantially all patient data, including, most egregiously, nude photos and videos of patients obtained during the course of treatment.

4. The hackers stole private personal and medical data from thousands of patients to use in an effort to extort Dr. Schwartz and the patients. During the first hack in or about September and October of 2023, the hacker group Hunters International downloaded 1.1 terabytes of patient data, reflecting almost 250,000 unique files. The private data included, among other things, nude photographs and video of patients, including images with both their faces and private parts visible, and images taken during surgery reflecting their surgical procedures.

5. Not only did Dr. Schwartz fail to notify his patients or law enforcement as required, but he actively hid the first hack from his patients. He also failed to take reasonable measures to secure his network, even after learning of the first hack.

6. Approximately six months later, in March of 2024, Dr. Schwartz's system was hacked again by a different hacker group. On information and belief, the second hacker group also gained access to his entire system and all or substantially all patient data. On information and belief, they successfully exfiltrated (*i.e.*, downloaded) over 1,700 patient files.

7. Once again, however, Dr. Schwartz attempted to sweep the second hack under the rug. He failed to notify his patients as required by federal and state law. He waited to do so until after the hackers posted a ***public website*** (the "Hacker Website"), announcing the hack and leaking patients' names, contact information, and nude photographs, and began contacting patients directly. Despite knowing that his patients' most private medical data was in the hands of malicious actors, Dr. Schwartz

waited almost 10 months to notify them. Finally, after their nude photos and home addresses began being posted online – accessible to anyone with an internet connection – and the hackers directly contacted patients to extort them, Dr. Schwartz issue a cursory, vague, and misleading data breach notice.

8. To date, the hackers have posted approximately 60 patient files, complete with names, dates of birth, phone numbers, home addresses, and nude photos – including photos of unconscious patients during surgery.[1] They have warned that they will continue releasing patient files until Dr. Schwartz's contacts them to address the matter.

9. In addition to the usual array of plastic surgery offerings, such as liposuction and breast augmentation, Dr. Schwartz specializes in treatment of lipedema. Lipedema is a painful and potentially disfiguring condition primarily affecting women. It involves the abnormal buildup of fat in the lower body, specifically the buttocks, thighs, and calves, as well as other areas.

10. Class Plaintiffs are patients of Dr. Schwartz and victims of the cyberattacks. They sought medically necessary treatment from Dr. Schwartz to address their lipedema on the understanding that their treatment and medical records would be kept strictly confidential. As a result of this treatment, Dr. Schwartz and his staff obtained extensive medical information about Class Plaintiffs and other patients, including the types of information, photographs, and videos outlined above. With respect to Class Plaintiffs and many others, these photographs and videos include detailed, nude and semi-nude images of their pelvic areas, breasts, thighs, and buttocks, including images and video taken during surgery.

11. On information and belief, all this information was exfiltrated from Dr. Schwartz's network during the recent cyberattack. All Class Plaintiffs have been threatened with the imminent release of this deeply private information. Two of the Class Plaintiffs already had their private data and images posted on the Hacker

[1] During the pendency of this action, the hackers have posted another 30 patient files.

Website. It is only a matter of time before the hackers reach all of their names in the alphabet and release their names, home addresses, medical information, and private images.

12. Plaintiffs bring this action for injunctive relief to rectify Dr. Schwartz's negligent cybersecurity practices and to require him to destroy or secure any private personal and medical information in his possession. They also seek statutory damages and damages for the severe emotional toll that having their private medical information compromised has taken on them.

PARTIES

Class Plaintiffs

13. Jane Doe 1 is an individual and citizen of the State of Colorado.

14. Jane Doe 2 is an individual and citizen of the State of Vermont.

15. Jane Doe 3 is an individual and citizen of the Commonwealth of Pennsylvania.

16. Jane Doe 4 is an individual and citizen of the State of California.

17. Jane Doe 5 is an individual and citizen of the State of New York.

18. Jane Doe 6 is an individual and citizen of the State of California.

19. Jane Doe 8 is an individual and citizen of the State of Oregon.

20. Jane Doe 9 is an individual and citizen of the State of California.

21. Jane Doe 10 is an individual and citizen of the State of Texas.

22. Jane Doe 11 is an individual and citizen of the State of California.

23. Jane Doe 12 is an individual and citizen of the State of California.

24. Jane Doe 13 is an individual and citizen of the State of Oklahoma

25. Jane Doe 14 is an individual and citizen of the State of Florida.

26. Jane Doe 15 is an individual and citizen of the State of Arizona.

27. Jane Doe 16 is an individual and citizen of the State of California.

28. Plaintiffs sue under these pseudonyms pursuant to *Does I through XXIII v. Advanced Textile Corp.*, 214 F.3d 1058, 1067 (9th Cir. 2000). Upon Defendants'

appearance in this action, Plaintiffs will promptly file a Motion with this Court to allow them to so proceed to protect their identities and the privacy of their medical information.[2]

Defendants

29. Defendant Jaime S. Schwartz, MD is an individual and, on information and belief, a resident of Los Angeles County, California. Dr. Schwartz owns and operates Jaime S. Schwartz, MD PC.

30. Defendant Jaime M. Schwartz, MD PC is a California professional corporation with its principal place of business in Beverly Hills, California. Jaime S. Schwartz, MD PC operates two plastic surgery practices in Beverly Hills and Dubai.

31. Defendant Karen L. Herbst, MD is an individual and, on information and belief, a resident of Arizona. At relevant times, Dr. Herbst was in practice with Dr. Schwartz, shared his computer network, stored patient data on his network, and sent patient data to Dr. Schwartz in connection with patient referrals, which data was also stored on his network. Dr. Herbst owns and operates Karen L. Herbst, MD, PC.

32. Defendant Karen L. Herbst, MD, PC, is a California professional corporation with its principal place of business in Beverly Hills, California. On information and belief, Karen L. Herbst, MD, PC, at all relevant times, shared offices, resources, and patients with Dr. Schwartz, and shared the use of Dr. Schwartz's computer network.

33. Defendant Total Lipedema Care is a California corporation with its principal place of business in Beverly Hills, California. On information and belief, Total Lipedema Care is jointly owned and controlled by Drs. Schwartz and Herbst, and was used as a vehicle to market medical services to and provide treatment to patients suffering Lipedema.

[2] Class Plaintiffs filed an Application to allow them to proceed anonymously on February 4, 2025. Dkt. No. 8. The Court declined to rule on the Application pending service on Defendants. Dkt. No. 9.

34. Class Plaintiffs are currently unaware of the true names and capacities of Defendants Does 1 through 10 ("Doe Defendants"), inclusive, and so name them under these fictitious names. Class Plaintiffs are informed and believe that the Doe Defendants are in some manner legally responsible for the acts, omissions, and damages alleged herein. On information and belief, the Doe Defendants include the individuals and entities who were in part responsible for maintaining the security of Dr. Schwartz's computer system and network, and the individuals and entities responsible for allowing the hack to take place. On information and belief, the Doe Defendants are principals, agents, partners, joint venturers, and alter egos of the other Defendants, acted in concert with the other defendants, aided and abetted the other Defendants, and conspired with the other Defendants in connection with the conduct alleged herein. Class Plaintiffs will seek leave to amend this Complaint to identify the true names and capacities of the Doe Defendants when the same become known.

JURISDICTION AND VENUE

35. This Court has subject matter jurisdiction pursuant to the Class Action Fairness Act, 28 U.S.C. § 1332. The amount in controversy in this action exceeds $5,000,000, exclusive of interests and costs. There are more than 100 members in the proposed class. Plaintiffs estimate that the data breaches affected hundreds, if not thousands, of Dr. Schwartz's patients. At least one member of the class is a citizen of a state different from Defendants, as set forth above.

36. The Court has personal jurisdiction over Defendants who maintain their residence and principal place of business in this District, and who regularly transact business within the State of California.

37. Venue is proper in this District pursuant to 28 U.S.C. § 1391 because a majority of the Defendants reside in this District and a substantial part of the events, acts, and omissions giving rise to Class Plaintiffs' claims occurred in and emanated from this District, namely from Defendants' primary office in Beverly Hills, California.

38. California has a significant interest in regulating businesses operating within its jurisdiction, including the protection of consumers' rights and personal data.

39. Defendants' operations are headquartered in Beverly Hills, California, from where Defendants oversee all corporate policies, including data security, from within the state. Based on available information, decisions regarding Defendants' network security and response to the data breach originated from California.

40. Because Defendants' actions and failures to act occurred in California, California's laws are appropriately applied. Under California's choice of law principles, California law governs the nationwide claims of Plaintiffs and the Class.

41. Additionally, California's Unfair Competition Law, CMIA, and Consumer Privacy Act apply to non-resident Plaintiffs due to Defendants' business operations in California and the fact that the acts and omissions from which liability arose occurred in California.

ALLEGATIONS COMMON TO ALL CLAIMS

Dr. Schwartz's and Dr. Herbst's Medical Practice

42. Dr. Schwartz owns and operates a plastic surgery practice in Beverly Hills, California. He is a board-certified plastic surgeon and a member of the American Society of Plastic Surgeons ("ASPS"). According to his marketing materials, he is "an internationally recognized expert in plastic surgery, specializing advanced surgical techniques" and "nationally renowned" for plastic surgery.

43. Dr. Schwartz offers a wide array of services, primarily catering to women. Among other things, he is widely known for his accomplishments in the field of breast augmentation and reconstruction, offering a host of related services to patients. He also offers a series of other surgical options focusing on private areas of the body, such as liposuction, butt lifts and implants, cellulite reduction, and vaginal rejuvenation.

44. In addition to a wide array of cosmetic surgeries, Dr. Schwartz also specializes in medically necessary treatment for lipedema. Lipedema treatment

involves highly invasive surgery to remove excess fat tissue from the buttocks, thighs, calves, and other areas, while preserving delicate lymph nodes and blood vessels.

45. Dr. Herbst also specializes in the treatment of lipedema. During the relevant period, Dr. Herbst and Dr. Schwartz worked together in treating patients with lipedema. Dr. Herbst also referred lipedema patients to Dr. Schwartz for surgery.

46. Dr. Herbst and Dr. Schwartz formed Total Lipedema Care to focus on marketing and providing lipedema treatment. The joint operation was headquartered at Dr. Schwartz's medical office in Beverly Hills. Both Dr. Herbst and Dr. Schwartz, and their respective medical corporations, shared office space and resources, and both used Dr. Schwartz's computer network to store patient data, including the data described herein. In addition, on information and belief, Dr. Herbst transmitted client data to Dr. Schwartz in connection with referring patients for surgery.

47. On information and belief, Dr. Herbst left the joint practice abruptly in or about late 2023 for unknown reasons. At that time, Dr. Herbst allowed Dr. Schwartz to retain patient medical and personal data, including photographs, on his network. On information and belief, Dr. Herbst did not take reasonable steps to ensure that the data was adequately secured either during the course of the joint practice, when referring patients to Dr. Schwartz, or when leaving the joint practice.

48. A material portion of the data exfiltrated during the two data breaches was data generated by or provided to Dr. Herbst in the course of treatment or consultation of her patients and stored on Dr. Schwartz's network.

Dr. Schwartz Maintains Extensive, Confidential Medical Information

49. By virtue of their treatment of Class Plaintiffs and other patients Defendants generated, received, and maintained a large volume of confidential and private information about their patients ("Personal and Medical Information").

50. This information includes, without limitation, patients' names, telephone numbers, and home addresses, their ages and dates of birth, their physical characteristics, including height, weight, eye color, and hair color, copies of their

driver's licenses and insurance cards, insurance information, *i.e.*, their insurance carriers and types of coverage, payment information, such as credit card information, and medical information, including medical history, conditions, diagnoses, and treatment.

51. Defendants also obtain from patients, generate, and maintain large numbers of photographs and videos depicting patients and their conditions. During the consultation process, both Drs. Schwartz and Herbst regularly ask that patients send in photos depicting their conditions. These photos are frequently nude or partially clothed.

52. In addition, Dr. Schwartz takes extensive photos and videos of patients during the course of treatment. He has an entire room at his surgery center dedicated to taking detailed photos completely documenting patients' physical condition before and after surgery. These photos are also frequently nude or partially clothed.

53. Finally, Dr. Schwartz and his staff film and photograph patients during surgery, ostensibly to allow Dr. Schwartz to document and review the surgery after it is completed. Class Plaintiffs' and other patients' faces are clearly visible in these photographs and video.

54. The photographs and videos are directly connected to Class Plaintiffs' and other patients' names and identifying information on Dr. Schwartz's network.

Defendants Were Obligated to Protect Personal Medical Information

55. Defendants are subject to the Health Insurance Portability and Accountability Act of 1996, Pub. L. No. 104-191, 110 Stat. 1936, as amended by the Health Information Technology for the Economic and Clinical Health Act, Pub. L. No. 111-5, 123 Stat. 226 ("HIPAA"). Among other things, Defendants are and were at all relevant times subject to the *Standards for Privacy of Individually Identifiable Health Information* (the "Privacy Rule") and the *Security Standards for the Protection of Electronic Protected Health Information* (the "Security Rule"), contained in 45 C.F.R. Parts 160 and 164, Subparts A and C. The Privacy Rule and the Security Rule

create nationwide standards for the protection of patient health information.

56. HIPAA required Defendants to "comply with the applicable standards, implementation specifications, and requirements" established under HIPAA "with respect to "electronic protected health information." 45 C.F.R. § 164.302.

57. The Security Rule required Defendants to do all of the following:

a. Ensure the confidentiality, integrity, and availability of all electronic protected health information the covered entity or business associate creates, receives, maintains, or transmits;

b. Protect against any reasonably anticipated threats or hazards to the security or integrity of such information;

c. Protect against any reasonably anticipated uses or disclosures of such information that are not permitted; and

d. Ensure compliance by their workforce.

58. HIPAA further required Defendants to "review and modify the security measures implemented … as needed to continue provision of reasonable and appropriate protection," 45 C.F.R. § 164.306(e), and to "[i]mplement technical policies and procedures for electronic information systems that maintain electronic protected health information to allow access only to those persons or software programs that have been granted access rights." 45 C.F.R. § 164.312(a)(1).

59. The California Confidentiality of Medical Information Act, Civil Code § 56, *et seq.* (the "CMIA"), also prohibits the disclosure of patient medical information without authorization. *See* Civ. Code § 56.10. "Medical information" is defined to include (a) individually identifiable information relating to a person's medical history, condition, or treatment, (b) in the possession of or derived from a provider of health care, (c) pertaining to a patient.

60. As "provider[s] of health care" as defined in the CMIA, Civ. Code § 56.05(f), Defendants were required to maintain medical information "in a manner that preserves the confidentiality of the information contained therein."

61. California Health and Safety Code § 1280.15 and 1280.18 require healthcare facilities to safeguard and prevent the unauthorized access of patient medical information.

62. Pursuant to California Civil Code § 1798.81.5(b), any "business that owns or licenses personal information about a California resident shall implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to protect the personal information from unauthorized access, destruction, use, modification, or disclosure."

63. Further, any business that discloses personal information "pursuant to a contract with a nonaffiliated third party shall require by contract that the third party implement and maintain reasonable security procedures and practices appropriate to the nature of the information, to prevent the personal information from unauthorized access." *Id.*, subd. (c).

64. In addition to the requirements of various statutes and regulations applicable to medical providers and holders of confidential consumer information, Defendants had a common law duty to Class Plaintiffs and other patients to use reasonable care in maintaining, securing, preserving, deleting, and protecting their Personal and Medical Information against the prevalent and well-known threat that it would be compromised, exfiltrated, and misused by unauthorized persons.

65. This duty included, without limitation, a duty to use reasonable security measures consistent with industry standards and requirements, and to ensure that computer systems, networks, and protocols adequately protected the Personal and Medical Information.

Defendants Had Ample Notice of the Risk of Cyberattacks and Industry Standards for Preventing Data Breaches.

66. Defendants were on notice of the risk of hacking in the medical field for years, and in the plastic surgery field in particular. They were also aware, or should have been aware, of the need to use best practices and take reasonable steps to protect

sensitive patient information. Defendants brazenly disregarded these standard practices, resulting in the two data breaches alleged herein.

67. For years, the medical community has been the target of hacking. The risk to patient data security posed by this hacking threat has been widely reported and is well known within the medical field.

68. In 2014, following the hack of Community Health Systems Inc., the FBI warned the medical profession that healthcare firms are targets for hackers. It specifically warned of the risk to patient data: "The FBI has observed malicious actors targeting healthcare related systems, perhaps for the purpose of obtaining Protected Healthcare Information (PHI) and/or Personally Identifiable Information (PII)." It is well known that patient medical data is highly valuable to hackers for purposes of extortion and ransom, making it a target for data breaches.

69. In 2019, the American Medical Association ("AMA") published a report entitled *Patient Safety: The Importance of Cybersecurity in Healthcare*, warning that cybersecurity "is not just a technical issue, it's a patient safety issue." The report noted that 83% of physicians had experienced some form of cyberattack. Among other risks, the AMA has warned physicians about the risks of ransomware attacks.

70. Since at least 2020, the American Medical Association ("AMA") has maintained a dedicated cybersecurity website, warning doctors and medical groups of the risks of hacking, including the risk to sensitive patient data, and providing industry standard guidelines for information security.

71. Similarly, since at least 2022, the U.S. Department of Health and Human Services ("DHHS") has maintained its own website on cybersecurity in the healthcare field, again warning of the risks of hacking and unauthorized access to private data.

72. Over the past several years, hackers have begun to focus their efforts on hacking plastic surgery practices due to the sensitive information retained by plastic surgeons. Multiple known and unknown hacker groups, including Hunters

International and Kairos, regularly target plastic surgery practices.[3]

73. Due to the nature of the data retained by plastic surgeons – *i.e.*, sensitive medical information and private and potentially embarrassing photographs – they are an attractive target. This information is particularly valuable for purposes of sale on the dark web and for extortion attempts against physicians and patients. Frequently these hacks have involved a hacker group gaining access to a surgeon's computer system and exfiltrating large amounts of sensitive patient data, including photographs. Hackers then use this data to attempt to extort the physician and/or patients directly.

74. According to a report from DataBreaches.net, between 2017 and 2023, there were at least a dozen publicly reported successful hacks of plastic surgery practices. Many of these hacks resulted in online data leaks and attempted extortion of surgeons or patients. Several high-profile plastic surgery practices were subject to hacks, such as the 2020 hack of the prominent Hospital Group, and the hacks were widely reported in the media.

75. The American Society of Plastic Surgeons ("ASPS"), of which Dr. Schwartz is a prominent member, has repeatedly warned its membership of the risks of hacking and published guidelines for cybersecurity.

76. Among other things, the ASPS publishes on its website a 2022 report co-authored by the DHHS and the Healthcare & Public Health Sector Coordinating Councils entitled *Health Industry Cybersecurity Practices: Managing Threats and Protecting Patients* ("DHHS Report"). This report warns of the serious risks of hacking on medical information systems and urges healthcare providers to adopt best practices to protect their systems. It notes, "Given the increasingly sophisticated and widespread nature of cyber-attacks, the health care industry must make cybersecurity a priority and make the investments needed to protect its patients."

[3] Some of these groups operate directly, and others offer "Ransomware-as-a-service" in which they license malicious software to third parties for a fee or a share of the ransom obtained through successful breaches. *See* Kurt Baker, *Ransomware as a Service (RaaS) Explained: How It Works & Examples*, CrowdStrike (Jan. 30, 2023).

77. In June of 2023, the hacking syndicate BlackCat (AlphV), publicly posted that they had hacked the well-known Beverly Hills Plastic Surgery, and "ha[d] lots of PII [patient identifying information] and PHI [protected health information], ***including a lot of pictures of patients that they would not want out there***." This hack was also publicly reported.

78. In the same timeframe, another well-known plastic surgeon in the Los Angeles area was hacked. When the surgeon refused to pay a $2.5 million ransom, the hackers began leaking nude photos of patients along with their personal identifying information, and threatened to leak more until the ransom was paid. The hackers also directly contacted patients and demanded $800,000 to remove their photos from a hacker website. This hack was also publicly reported.

79. On July 6, 2023, the ASPS sent an alert to its membership, entitled *Notice of ransomware scam targeting plastic surgeons*, about the risk of ransomware "phishing" attacks. The alert warned that hackers had targeted plastic surgeons, and having gained access to the surgeons' systems, "***comb[] the surgeon's network for patient data and photos***. This then leads to an extortion attempt to release that data."

80. The hacking threat against plastic surgeons has become so significant that in October of 2023, the FBI issued a Public Service Announcement, entitled *Cybercriminals are Targeting Plastic Surgery Offices and Patients*, Alert Number: I-101723-PSA, warning surgeons of the risk of hacking. The Public Service Announcement again warned that cybercriminals were actively targeting plastic surgery offices "*to harvest personally identifiable information and sensitive medical records,* ***to include sensitive photographs*** in some instances."

81. The announcement explained the process of these hacks, including:

a. "Data Harvesting," including "harvest[ing] electronically protected health information (ePHI), which includes sensitive information and photographs";

b. "Data Enhancement," using publicly available information, such as social media, to gather additional information about patients to use in extortion; and

c. "Extortion," demanding money from surgeons and patients to prevent disclosure of the sensitive data.

82. The announcement noted that, "[t]o exert pressure on victims for extortion payments, cybercriminals share the sensitive ePHI to victims' friends, family, or colleagues, and create public-facing websites with the data. Cybercriminals tell victims they will remove and stop sharing their ePHI only if an extortion payment is made."

83. On October 19, 2023, the ASPS reposted the FBI Public Service Announcement on its website.

October 2023—The First Hack and Failed Response

84. On information and belief, in September or October 2023, the hacker group Hunters International successfully hacked Dr. Schwartz's network (the "First Hack"). The group took credit for the successful hack on the dark web.

85. According to its dark web posting, Hunters International had exfiltrated 1.1 terabytes of data from Dr. Schwartz, consisting of 248,245 files. Based on publicly available data, the dark web posting included four patient photos, including one nude photo with the patient's face visible. The hackers claimed that they had hacked Dr. Schwartz's system in September of 2023.

86. On November 11, 2023, Hunters International updated their dark web posting by listing patient data and included the following note to Dr. Schwartz:

> Seems like you don't want to protect your data at all. More than 30 days had passed already since your network has been breached. You have been provided with everything you have asked about: sample of files, decryption tool demonstration, filetree, personal details. But you keep begging for proofs. This is not the way we going to make business with you. Maybe you will do us a favor and transfer half of the money to prove that you can pay for your data? That would be fair, we guess. **Nevertheless, we will start deploying a little piece of your data everyweek, until all of your data will be shared this way. Starting today. You still have an option to pay for your data, until sharing is finished.**

87. On December 1, 2023, Hunters International reposted its dark web

listing, this time adding nude photos of patients, and advising, "If you find your private data here just email us and we will let you know how to proceed further with actions against this DOCTOR!"

88. Dr. Schwartz did not notify patients of the September/October 2023 attack. He unequivocally refused to pay ransom. On information and belief, he also failed to provide required notices to the California Attorney General or the DHHS.

89. Instead, when a small number of patients contacted Dr. Schwartz after the First Hack was reported online, he and his staff attempted to minimize the data breach by falsely claiming that it affected only a small number of patients and that other patients' records were secure. Dr. Schwartz and his colleagues continued to assure patients (falsely) that their data was not compromised.

90. Eventually, Hunters International posted all or substantially all of the exfiltrated data on its dark web "leak" site, organized by client name.

March 2024—The Second Hack and Dr. Schwartz Untimely Disclosure

91. Despite hackers compromising his system and attempting to extort him, Dr. Schwartz still failed to implement reasonable security protocols.

92. In early 2024, Dr. Schwartz's system was hacked a second time (the "Second Hack"; collectively with the First Hack, "Data Breaches") by a different hacker group, operating under the name "Boobs & Pussies."

93. Dr. Schwartz claims that he first learned of this hack in late June 2024 but, on information and belief, he learned of the second hack much earlier.

94. It is unclear how long his system had been compromised before he purportedly "discovered" the Second Hack. According to the Hacker Site – a public, "clear web" site[4] posted by the hackers – they successfully compromised Dr. Schwartz's system in March of 2024.

[4] The "clear web" or "surface web" refers to the publicly accessible internet, indexed by standard search engines, such as Google. It is distinguished from the "dark web" which must be accessed through specialized software.

95. The hackers again obtained large amounts of sensitive patient data, including the data of the Class Plaintiffs. On information and belief, the hackers exfiltrated Personal and Medical Information of at least hundreds of patients. The data breach included data from patients of both Dr. Schwartz and Dr. Herbst.

96. This data included patient's full names, identifying information, home addresses, dates of birth, and physical data, as well as insurance information and payment information regarding procedures not covered by insurance. According to Dr. Schwartz's belated notice of the data breach, the affected data also included medical information and prescription medications. Most disturbingly, it included nude and partially clothed photographs and videos, including photographs during surgery.

97. On or about December 16, 2024, the hackers posted the Hacker Website, announcing the hack and disclosing that Dr. Schwartz had refused to address the incident for months. The website includes extremely sensitive data, including personally identifying information of patients and nude photos taken during surgery. The hackers also threaten on the website to continue releasing information and photos of additional patients if Dr. Schwartz does not contact them.

98. To date, the hackers have published sensitive personal information of 60 patients, organized by name and data of birth. The files include headshots of the victims, full, unredacted copies of their drivers' licenses and insurance cards, and nude and partially clothed photos, depicting their medical conditions and surgeries. Some of the photos appear to have been taken while patients were unconscious and undergoing surgery, reflecting surgical incisions and sutures.

99. The hackers have continued posting patient data and images online since the filing of this action.

100. Once again, on information and belief, Dr. Schwartz failed to take reasonable steps to secure his system, and he failed to respond in an appropriate manner to the second hack as required by law.

101. In January of 2025, Dr. Schwartz sent certain patients, including Class

Plaintiffs, a Notice of Data Security Incident (the "Data Breach Notice"). In it, he notified patients as follows:

> Our office discovered on June 27, 2024, that an unauthorized third party utilized a third-party vendor's credentials to access the practice's medical billing and practice management system. Upon discovering the incident, we engaged a specialized third-party forensic incident response firm to conduct a forensic investigation and determine the extent of the compromise. The investigation determined that data was acquired without authorization. After electronic discovery, which concluded on January 2, 2025, it was determined that some of your personal information was present in the impacted data set. We then took steps to notify you of the incident as quickly as possible.

102. Dr. Schwartz failed to timely notify the California Attorney General or the DHHS as required by law. He notified the California Attorney General only after the filing of this lawsuit and, on information and belief, has not notified the DHHS.

103. Because Dr. Schwartz has not yet made a full or transparent disclosure of the hack, significant questions remain about the nature and scope of the hack and the types and amounts of data that have been compromised. Plaintiffs are informed and believe, however, that the hackers gained access to, viewed, and/or copied substantially all of the patient data on Dr. Schwartz's system.

Dr. Schwartz Negligently Maintained His Systems

104. The Data Breaches were caused by Defendants' negligence in retaining patient data and failing to secure the network and computer systems, which allowed malicious actors to gain access to those systems and to access and exfiltrate unencrypted Personal and Medical Information.

Prevailing Standards for Protection of Sensitive Patient Data

105. Governmental agencies, industry organizations, and technology companies have established a set of basic cybersecurity standards to minimize the risk of hacking and access to unencrypted patient or customer data.

106. For example, the DHHS Report provides the following basic cybersecurity protocols for the medical industry, among others:

a. securing email accounts;

b. installing and maintaining spam/anti-virus software solutions;

c. using multi-factor authentication (MFA);

d. correctly configuring security settings;

e. training employees on cybersecurity;

f. limiting user access to administrative accounts so that administrative accounts are used only for essential purposes;

g. utilizing encryption on user devices;

h. enabling network firewalls;

i. utilizing MFA for access to connected devices;

j. maintaining unique user accounts and tailoring each user's access to essential functionality and data;

k. using encrypted storage media and devices for sensitive information;

l. controlling access to sensitive and highly sensitive data within the network, including placing more sensitive data in restricted zones that are more difficult to access;

m. limiting third-party vendor access to sensitive data;

n. establishing and enforcing network "traffic" restrictions;

o. monitoring network activity and maintaining an audit trial, and

p. monitoring and patching vulnerabilities and keeping software updated.

107. The FBI recommends the following security measures, among others:

a. Implement an awareness and training program. Because end users are targets, employees and individuals should be aware of the threat of ransomware and how it is delivered.

b. Enable strong spam filters to prevent phishing emails from reaching the end users and authenticate inbound email using technologies like Sender

Policy Framework (SPF), Domain Message Authentication Reporting and Conformance (DMARC), and DomainKeys Identified Mail (DKIM) to prevent email spoofing.

c. Scan all incoming and outgoing emails to detect threats and filter executable files from reaching end users.

d. Configure firewalls to block access to known malicious IP addresses.

e. Patch operating systems, software, and firmware on devices. Consider using a centralized patch management system.

f. Set anti-virus and anti-malware programs to conduct regular scans automatically.

g. Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.

h. Configure access controls-including file, directory, and network share permissions-with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.

i. Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.

j. Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.

k. Consider disabling Remote Desktop protocol (RDP) if it is not being used.

l. Use application whitelisting, which only allows systems to execute

programs known and permitted by security policy.

m. Execute operating system environments or specific programs in a virtualized environment.

n. Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.

108. The United States Cybersecurity & Infrastructure Security Agency recommends the following protective measures, among others:

a. Update and patch your computer. Ensure your applications and operating systems (OSs) have been updated with the latest patches. Vulnerable applications and OSs are the target of most ransomware attacks....

b. Use caution with links and when entering website addresses. Be careful when clicking directly on links in emails, even if the sender appears to be someone you know. Attempt to independently verify website addresses (e.g., contact your organization's helpdesk, search the internet for the sender organization's website or the topic mentioned in the email). Pay attention to the website addresses you click on, as well as those you enter yourself. Malicious website addresses often appear almost identical to legitimate sites, often using a slight variation in spelling or a different domain (e.g., .com instead of .net)....

c. Open email attachments with caution. Be wary of opening email attachments, even from senders you think you know, particularly when attachments are compressed files or ZIP files.

d. Keep your personal information safe. Check a website's security to ensure the information you submit is encrypted before you provide it....

e. Verify email senders. If you are unsure whether or not an email is legitimate, try to verify the email's legitimacy by contacting the sender directly. Do not click on any links in the email. If possible, use a previous (legitimate) email to ensure the contact information you have for the sender is authentic before you contact them.

f. Inform yourself. Keep yourself informed about recent cybersecurity threats and up to date on ransomware techniques….

g. Use and maintain preventative software programs. Install antivirus software, firewalls, and email filters-and keep them updated-to reduce malicious network traffic...

109. The Microsoft Threat Protection Intelligence Team, an industry leader in cybersecurity, recommends the following practices:

a. Secure internet-facing assets;

b. Apply latest security updates;

c. Use threat and vulnerability management;

d. Perform regular audits;

e. Remove privileged credentials

f. Thoroughly investigate and remediate alerts;

g. Prioritize and treat commodity malware infections as potential full compromise;

h. Include IT Pros in security discussions

i. Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

j. Build credential hygiene

k. Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords;

l. Apply principle of least-privilege;

m. Monitor for adversarial activities;

n. Hunt for brute force attempts;

o. Monitor for cleanup of Event Logs;

p. Analyze logon events;

q. Harden infrastructure;

r. Use Windows Defender Firewall;

s. Enable tamper protection;

t. Enable cloud-delivered protection;

u. Turn on attack surface reduction rules and [Antimalware Scan Interface] for Office [Visual Basic for Applications].

Defendants' Failure to Implement Reasonable Protections

110. Defendants failed to implement and maintain reasonably adequate cybersecurity protocols, which failure allowed and exacerbated the Data Breaches. On information and belief, their negligent failures to protect patient data included, without limitation, the following.

111. Defendants failed to store highly sensitive patient data in appropriately secured parts of their network consistent with the sensitivity of the data and, on information and belief, stored patient data in an unencrypted format or with inadequate encryption in place. In addition, Defendants allowed sensitive patient data, including photographs, videos, and medical information, to be stored on unused and obsolete systems, and outside of a secured network, and allowed those systems to remain accessible after they were no longer in use.

112. Defendants failed to adequately secure patient files to prevent them from being accessible over the internet.

113. Defendants failed to properly manage access to their system, including failing to implement appropriate multi-factor authentication for staff and vendors, gave staff and vendors access to information that was not necessary to perform their functions, failed to enforce appropriate credential hygiene – *e.g.*, regular password changes –, and failed to ensure that users had appropriate, strong passwords. Defendants also failed to adequately restrict user access to network resources and data for which those users had no legitimate need and stored sensitive patient data that allowed access by user accounts without a legitimate need for access.

114. Defendants failed to secure network-connected devices, including

connected medical devices, in a manner reasonably designed to prevent intrusion.

115. Defendants failed to adequately train their staff to avoid "phishing" and other social-engineering attacks, failed to use due care in selecting and supervising third-party vendors, and failed to reasonably ensure that vendors with access to sensitive patient data were appropriately retained and maintained secure access credentials.

116. Defendants utilized third-party applications, such as patient-communication platforms, to store and/or access sensitive data, without adequate security measures in place to ensure that such platforms were not subject to cyberattack.

117. Defendants failed to adequately monitor network traffic or suspicious network activity as necessary to prevent or promptly discovery malicious activity, and failed to implement appropriate network "traffic" controls to prevent the exfiltration of large amounts of data. Defendants also failed to use appropriate anti-malware software and firewalls to prevent and detect suspicious network activity and failed to appropriately train staff to detect suspicious activity and avoid or mitigate the risk of malicious activity on the network.

The Impact of the Cyberattacks on Class Plaintiffs

Jane Doe 1

118. Jane Doe 1 saw Dr. Schwartz for three medically necessary lipedema surgeries between 2021 and 2022, which took place in California. Through the course of this treatment, Defendants obtained, generated, and maintained extensive Personal and Medical Information about Jane Doe 1, including her name, address, date of birth, phone number, insurance information, and copies of her driver's licenses and insurance card. In addition, Dr. Schwartz obtained and stored private images of Jane Doe 1 in a nude or semi-clothed state for purposes of medical treatment, including images that show Jane Doe 1's face as well as her lipedema. In addition, Dr. Schwartz obtained and maintained in his electronic files fully nude videos of Jane Doe 1.

119. Jane Doe 1 is informed and believes that all or substantially all of her private data in Defendants' possession was compromised and exfiltrated through the Data Breaches. She faces an imminent risk of dissemination and/or misuse of her confidential data, including sensitive images.

120. Dr. Schwartz failed to inform Jane Doe 1 of the First Hack in any manner although, on information and belief, her confidential Personal and Medical Information was compromised. In or about January of 2025, Jane Doe 1 found out about the Second Hack through a social media group for women suffering from lipedema. At that time, she also learned of the First Hack. She subsequently received a copy of the Data Breach Notice from Dr. Schwartz relating to the Second Hack on or about February 1, 2025.

121. Jane Doe 1 has suffered severe emotional distress as a result of the data breaches. She lives in constant fear that malicious actors will either disclose her data publicly on the Hacker Website or elsewhere, or will use that data for nefarious purposes, including identity theft. Jane Doe 1 has suffered fear, embarrassment, humiliation, shame, anxiety, and depression as a result of her private data and photographs being compromised. She has begun to suffer headaches, nausea and vomiting, and fatigue, as well as difficult concentrating. She is afraid of going out in public and being recognized from the images taken from Dr. Schwartz's system, and fears opening her email and other forms of electronic communication to discover that she has been contacted by the hackers. The emotional and physical symptoms caused by the Data Breaches have affected her ability to perform basic life activities.

Jane Doe 2

122. Jane Doe 2 saw Dr. Schwartz for five medically necessary surgeries for treatment of lipedema between 2022 and 2023, which took place in California. Through the course of treatment, Defendants obtained, generated, and maintained extensive Personal and Medical Information about Jane Doe 2, including her name, address, date of birth, phone number, insurance information, payment information,

and copies of her driver's licenses and insurance card. In addition, Dr. Schwartz obtained and stored private images of Jane Doe 2 in a nude or semi-clothed state for purposes of medical treatment, including images that show Jane Doe 2's face as well as her lipedema.

123. Jane Doe 2 is informed and believes that all or substantially all of her private information in Defendants' possession was accessed and exfiltrated during the Data Breaches. She faces an imminent risk of dissemination and/or misuse of her confidential data.

124. In or about January of 2025, Jane Doe 2 learned about the Second Hack through an online group for women suffering from lipedema. Through this group she learned that there was a public website with information and photographs of Dr. Schwartz's patients, and that more patient information was being released in alphabetical order. Jane Doe 2 subsequently received a Data Breach Notice dated January 15, 2025 from Dr. Schwartz.

125. To mitigate the risk of identity theft, Jane Doe 2 signed up for an online identity protection service for which she is personally paying.

126. She has also suffered severe emotional distress as a result of the Data Breaches, including fear, humiliation, anxiety, and a sense of impending doom. She has begun suffering nausea and headaches after learning of the data breach and has difficulty sleeping. In the weeks after she learned about the data breach, it was all Jane Doe 2 thought about, and she had difficulty concentrating on anything else. She fears going out in public and being recognized, and fears opening her emails and electronic communications.

Jane Doe 3

127. Jane Doe 3 had five surgeries with Dr. Schwartz between 2020 and 2021, which took place in California. Through the course of this treatment, Defendants obtained, generated, and maintained extensive Personal and Medical Information about Jane Doe 3, including her name, address, date of birth, phone number, insurance

information, personal payment information, and copies of her driver's licenses and insurance card. In addition, Dr. Schwartz obtained and stored private images of Jane Doe 3 in a semi-clothed and topless state for purposes of medical treatment, including images with Jane Doe 3's face visible.

128. Jane Doe 3 is informed and believes that all or substantially all of the Personal and Medical Information in Defendants' possession was accessed and exfiltrated during the Data Breaches. She faces an imminent risk of dissemination and/or misuse of her confidential data.

129. She learned of the Second Hack in or about January of 2025 through a Facebook group for women suffering from lipedema. After learning of the Second Hack through this group, she began researching online and found out about the First Hack. Dr. Schwartz never informed her of the First Hack. Through her online research, she also found the Hacker Website where other patients' photos and data had been posted as a result of the data breach. Dr. Schwartz sent Jane Doe 3 a Data Breach Notice in January of 2025.

130. Jane Doe 3 has spent many hours attempting to mitigate the harm caused by the Data Breaches, including researching the Data Breaches online, researching ways to protect her identity, and communicating with other victims about strategies to protect her private data from disclosure. She has been notified three times since the First Hack that her name now appears on the dark web.

131. Jane Doe 3 constantly worries about the misuse of her information as a result of the Data Breaches, such as someone googling her name and finding semi-clothed or topless images of her online, or someone stealing her identity. Her anxiety over the data breach has distracted her from other life activities, such as engaging with loved ones, and resulted in difficulty concentrating on other things. She suffers fear, embarrassment, humiliation, depression, and a sense of impending doom as a result of the data breach, as well as nausea, headaches, fatigue, and insomnia. The incident has caused Jane Doe 3 to be distrustful of doctors and other medical professionals and has

caused concern about seeking other medical treatment. Jane Doe 3 fears being recognized from the topless photographs exfiltrated from Dr. Schwartz's system.

Jane Doe 4

132. Jane Doe 4 began seeing Dr. Schwartz in 2020 and had a surgery at his California office in July of 2024. Throughout her consultations with him, Dr. Schwartz's staff took unclothed photographs of her.

133. In the interim, Dr. Schwartz's system was compromised. Without informing Jane Doe 4 of the Data Breaches, Dr. Schwartz continued to obtain confidential medical information from Jane Doe 4, including her medical history, contact information, driver's license, medical insurance card, diagnoses, and list of medications. He also received, took, and maintained sensitive photographs of Jane Doe 4, reflecting her lipedema, including photographs with her face visible. All of this private Personal and Medical Information was stored on his computer network.

134. Dr. Schwartz performed surgery on Jane Doe 4 at his Beverly Hills, California office in July of 2024 mere weeks after he purportedly found out that he had been hacked for a second time. Despite later admitting that he had knowledge of the Second Hack at the time of Jane Doe 4's surgery, Dr Schwartz did not notify Jane Doe 4 of the breach, nor, that her private data was compromised. Instead, he proceeded to have his staff take photographs and video of Jane Doe 4 during PreOp, PostOp, and on the operating table during surgery.

135. On information and belief, the hackers compromised and downloaded all of Jane Doe 4's data in Dr. Schwartz's possession. Jane Doe 4 faces an imminent threat of misuse and/or public release of her Personal and Medical Information.

136. Jane Doe 4 has spent numerous days attempting to mitigate her damage, including researching the Data Breaches and potential mitigation strategies, contacting Dr. Schwartz, contacting law enforcement, and coordinating with other victims.

137. The Data Breaches have caused severe emotional distress to Jane Doe 4, and she is currently in therapy for the emotional harm caused by Defendants' conduct.

Jane Doe 4 has a pre-existing medical condition that causes occasional panic attacks, which have become more frequent and affected her quality of life. After she learned of the Data Breaches, she has lived in constant fear, anxiety, and depression, and has been required to take prescription medication to help control the emotional impact. She is unable to sleep, and her insomnia has not responded to medication. She feels fear, humiliation, embarrassment, shame, and a sense of impending doom. The emotional distress has manifested in physical symptoms, including insomnia, nausea, and fatigue. Jane Doe 4 fears opening her emails and electronic communications and being contacted by the hackers and has received a series of strange phone calls and texts since the Second Hack. The Data Breaches have consumed Jane Doe 4's thoughts, making it impossible for her to concentrate on other activities, and have severely impacted her daily life.

Jane Doe 5

138. Jane Doe 5 saw Dr. Schwartz for three medically necessary lipedema surgeries and a follow-up procedure between 2022 and 2023. Dr. Schwartz performed the surgeries and the procedure in his office in Beverly Hills, California. Jane Doe 5 continued her consultation with Dr. Schwartz and his staff thereafter. At all relevant times, Dr. Schwartz and his staff were in California.

139. Through the course of her treatment, Defendants obtained, generated, and maintained significant amounts of Personal and Medical Information regarding Jane Doe 5. This information included, without limitation, Jane Doe 5's personal identifying information, her insurance information, and her medical history, conditions, and diagnoses. It also included a large number of nude and partially clothed photographs documenting Jane Doe 5's condition and the progress of her treatment.

140. On information and belief, during the Data Breaches, hackers gained access to and exfiltrated Jane Doe 5's confidential information. Jane Doe 5 faces a risk of imminent release of her personally identifying and private medical information

as a result of the Data Breaches.

141. Jane Doe 5's son discovered articles about the First Hack online. In early 2024, Jane Doe 5 contacted Dr. Schwartz to inquire about the data breach and whether her medical information was compromised. Thereafter, a person claiming to be in charge of cybersecurity for Dr. Schwartz called Jane Doe 5. Jane Doe 5 is informed and believes that the person was Dr. Schwartz's brother.

142. The individual claimed (falsely) that the data breach had affected only approximately six patient files and that Defendants had stopped the hackers before they gained significant access to Defendants' network. He further claimed that Dr. Schwartz was working with the FBI and had completely overhauled the computer system to prevent future cyberattacks. The individual also assured Jane Doe 5 that her information was safe and had not been compromised. On information and belief, these representations were false and intended to dissuade Jane Doe 5 from taking action in response to the security breach.

143. In or about December of 2024, Jane Doe 5 learned of the Second Hack through a post to an online forum. She attempted to contact Dr. Schwartz, but he was not returning phone calls. She received no further communication from Dr. Schwartz until receiving a generic Data Breach Notice in or about January of 2025.

144. Jane Doe 5 has suffered severe emotional distress as a result of the Data Breaches, including fear, embarrassment, humiliation, a sense of impending doom, anxiety, and depression not only due to the violation of her medical privacy but also the violation of the trust she placed in Dr. Schwartz. As a consequence of the Data Breaches, Jane Doe 5 has difficulty concentrating and fears opening her emails and other electronic communications, which has affected her ability to engage in ordinary daily activities.

Jane Doe 6

145. Jane Doe 6 underwent two medically necessary surgeries by Dr. Schwartz in 2021 to treat lipedema. During the course of treatment, Defendants

obtained Jane Doe 6's private information, including her personally identifying information, insurance information, and medical information. They also obtained photographs and videos of Jane Doe 6 both before and during surgery. All of Jane Doe 6's medical data was stored on Defendants' network.

146. Jane Doe 6 is informed and believes that all or substantially all of her medical information, photographs, and videos were accessed and exfiltrated during the Data Breaches. Jane Doe 6 faces a risk of imminent release of her personally identifying and private medical information as a result of the Data Breaches.

147. Jane Doe 6 first learned of the Data Breaches in late December 2024 or early January 2025 through other victims. In or about January of 2025, Jane Doe 6 received the generic Data Breach Notice from Dr. Schwartz.

148. Jane Doe 6 has suffered severe emotional distress as a result of the Data Breaches. She remains concerned that her personal, medical, and financial information has been or may be misused.

Jane Doe 8

149. Jane Doe 8 saw Dr. Schwartz for five medically necessary surgeries to treat her lipedema and for skin excisions. She is active online in the lipedema community.

150. During the course of treatment, Dr. Schwartz and his staff obtained a large volume of Personal and Medical Information regarding Jane Doe 8. Among other things, Defendants obtained Jane Doe 8's identifying information, insurance information, and medical information, including conditions, diagnoses and treatments. Defendants also obtained and generated photographs of Jane Doe 8 in a nude and/or partially clothed state during the course of treatment.

151. On information and belief, all of Jane Doe 8's Personal and Medical Information was stored on Defendants' computer network. As a result, all of that information was compromised in the Data Breaches. Jane Doe 8 faces an imminent risk that her private information will be misused or publicly disclosed.

152. Jane Doe 8 has been severely affected by the Data Breaches. She operates an online business and fears that if her private medical information is disclosed, it will damage her business prospects. She has also suffered shame, embarrassment, and humiliation as a result of the Data Breaches.

Jane Doe 9

153. Jane Doe 9 saw both Dr. Schwartz and Dr. Herbst through Total Lipedema Care for treatment of lipedema.

154. During the course of treatment Drs. Schwartz and Herbst solicited partially clothed photos from Jane Doe 9, including partially clothed photos reflecting her medical condition. At their request, Jane Doe 9 uploaded the photos through Defendants' online portal.

155. On information and belief, all of Jane Doe 9's Personal and Medical Information was stored on Defendants' computer network and was compromised in the Data Breaches and exfiltrated through the online system.

156. Jane Doe 9's Personal and Medical Information has been publicly leaked on the public Hacker Website, including personally identifying information, medical insurance information, and partially clothed photographs depicting Jane Doe 9's face and body.

157. Dr. Schwartz failed to provide Jane Doe 9 a notice of the data breach until after the filing of this lawsuit.

158. Jane Doe 9 has been severely affected by having her private Personal and Medical Information compromised and leaked online. Jane Doe 9 now lives in constant fear that future employers, insurance companies, or others will find her personal and private information (including photographs) online. She has suffered shame, embarrassment, fear, humiliation, and anxiety with physical symptoms.

Jane Doe 10

159. Jane Doe 10 was a patient of both Dr. Schwartz and Dr. Herbst and received medically necessary treatment for lipedema.

160. During the course of treatment, Dr. Herbst, Dr. Schwartz, and their respective staff received a large volume of Personal and Medical Information from Jane Doe 10. Among other things, Defendants obtained Jane Doe 10's identifying information, medical information (including conditions, diagnoses, and treatments), insurance information, and photographs of Jane Doe 10 in a nude and/or partially clothed state.

161. On information and belief, all of Jane Doe 10's Personal and Medical Information was stored on Defendants' computer network. As a result, all of that information was compromised in the Data Breaches. Jane Doe 10 faces an imminent risk that her private information will be misused or publicly disclosed.

162. Jane Doe 10 has been severely affected by the Data Breaches. Due to the hackers leaking patient data on an ongoing basis, she fears that her personal and private information, including her photographs, will be leaked online where it will be seen by friends, colleagues, family members, and others. Jane Doe 10 has suffered stress, anxiety, worry, shame, embarrassment, and humiliation as a result of the Data Breaches.

Jane Doe 11

163. Jane Doe 11 sought medically necessary treatment from Dr. Schwartz for lipedema.

164. During the course of seeking treatment, Jane Doe 11 provided photographs to Dr. Schwartz at his request and Dr. Schwartz took photos of Plaintiff, including fully nude photos. In addition, Dr. Schwartz obtained other Personal and Medical Information pertaining to Jane Doe 11, including a copy of her driver's license and insurance information.

165. On information and belief, all of Jane Doe 11's Personal and Medical Information was stored on Defendants' computer network and was compromised in the Data Breaches. Jane Doe 11 faces an imminent risk that her private information will be misused or publicly disclosed.

166. Dr. Schwartz did not notify Jane Doe 11 that her Personal and Medical Information had been compromised. Instead, Jane Doe 11 learned of the Data Breaches from another patient.

167. Jane Doe 11 has been severely affected by the Data Breaches. She has suffered fear, embarrassment, shock, anxiety, and depression, along with physical symptoms such as insomnia, nausea, chest pain, and heart palpitations due to fear of her personal information and photographs being leaked online. Jane Doe 11 has spent more than 20 hours attempting to address the Data Breaches, including investigating the breaches and reporting to law enforcement. She has also incurred expenses for a data monitoring service.

Jane Doe 12

168. Jane Doe 12 saw Dr. Schwartz for surgery in 2016.

169. During the course of treatment, Dr. Schwartz's staff took nude photographs of Plaintiff as well as photographs and video during surgery. Dr. Schwartz stored the photographs on a patient portal available online. In addition, Dr. Schwartz obtained other Personal and Medical Information pertaining to Jane Doe 12.

170. On information and belief, Jane Doe 12's Personal and Medical Information was stored on Dr. Schwartz's system and compromised during one or both of the Data Breaches.

171. Dr. Schwartz did not send Jane Doe 12 any notice of the Data Breaches.

172. Jane Doe 12 has been severely affected by the Data Breaches. She fears that her private data, including the details of her surgery and nude photographs/video will be leaked online and seen by friends, family members, colleagues, or others in her industry, damaging her career prospects. Jane Doe 12 has suffered fear, embarrassment, humiliation, shock, anxiety, and depression with physical symptoms.

Jane Doe 13

173. Jane Doe 13 received medically necessary treatment from Dr. Schwartz for lipedema.

174. During the course of treatment, Dr. Schwartz obtained Personal and Medical Information from Jane Doe 13. Among other things, at Dr. Schwartz's request, Jane Doe 13 submitted post-procedure photographs through a series of online portals maintained by Dr. Schwartz. In addition, Dr. Schwartz took photos and/or video of Jane Doe 13 during surgery.

175. Jane Doe 13's Personal and Medical Information was stored on Dr. Schwartz's system and was compromised during one or both of the Data Breaches.

176. In February of 2025, Dr. Schwartz sent Jane Doe 13 the generic data breach notice described above.

177. Jane Doe 13 has been seriously affected by the Data Breaches. She is self-employed in a highly competitive field and fears damage to her reputation if her images and medical information are leaked. She has suffered fear, embarrassment, humiliation, a sense of betrayal, anxiety, and depression with physical symptoms.

Jane Doe 14

178. Jane Doe 14 sought medically necessary treatment from Dr. Schwartz for lipedema. During the course of treatment, Dr. Schwartz obtained and generated a large volume of Personal and Medical Information regarding Jane Doe 14, including nude photographs, partially nude photographs, and photographs and/or videos taken while Jane Doe 14 was undergoing surgery. In addition, Dr. Schwartz obtained Jane Doe 14's personally identifying information, insurance information, and payment information.

179. Dr. Schwartz stored Jane Doe 14's Personal and Medical Information on his system. As a result, that Personal and Medical Information was compromised during the Data Breaches.

180. Jane Doe 14 was confused and mislead by the generic Data Breach Notice sent by Dr. Schwartz, and erroneously assumed that ordinary consumer information was compromised, not private medical information, such as photographs.

181. After learning of the nature of the Data Breaches, Jane Doe 14 has spent

several hours researching the Data Breaches to find out the extent of those breaches and whether her information has been leaked. She has suffered fear, embarrassment, humiliation, shock, and anxiety with physical symptoms, including nausea and panic attacks.

Jane Doe 15

182. Jane Doe 15 received medically necessary treatment from Drs. Schwartz and Herbst for lipedema.

183. During the course of treatment, Drs. Schwartz and Herbst obtained Personal and Medical Information from Jane Doe 15. Among other things, at Dr. Schwartz's request, Jane Doe 15 submitted post-procedure photographs through a series of online portals maintained by Dr. Schwartz. In addition, Dr. Schwartz took photos and/or video of Jane Doe 15 during surgery and during pre- and post-operative visits. Dr. Herbst took photographs of Jane Doe 15 during a visit as well.

184. Jane Doe 15's Personal and Medical Information was stored on Dr. Schwartz's system and was compromised during one or both of the Data Breaches.

185. In or around February of 2025, Dr. Schwartz sent Jane Doe 15 the generic Data Breach Notice described above.

186. Jane Doe 15 has been seriously affected by the Data Breaches. She has suffered fear, embarrassment, humiliation, a sense of betrayal, anxiety, and depression with physical symptoms. The fear of her personal information and private and exposing images becoming public has significantly impacted her emotional and psychological condition and has diminished her ability to enjoy life and participate in daily tasks and activities

Jane Doe 16

187. Jane Doe 16 consulted with Dr. Herbst regarding medically necessary lipedema treatment in 2023. At Dr. Herbst's request, Jane Doe 16 obtained copies of her photographs from her surgeon and transmitted them to Dr. Herbst. Jane Doe 16

also provided other Personal and Medical Information, including identifying information, medical information, insurance information, and payment information. Jane Doe 16 is informed and believes that after her information was transmitted to Dr. Herbst, it was stored on Dr. Schwartz and Dr. Herbst's shared computer network and compromised in the Second Hack.

188. In late 2024, Jane Doe 16 received a call from an individual who identified himself as one of the hackers who had compromised Dr. Schwartz's network. The hackers have since called and text messaged Jane Doe 16 repeatedly, attempting to extort her. They have stated that they have nude images, and that images have been posted on the Hacker Website. The hackers have demanded money to remove the images from the Hacker Website.

189. Jane Doe 16's personal information, including identifying information, insurance information, and partially clothed photographs with her face and body visible, have been posted on the Hacker Website.

190. Jane Doe 16 has been severely affected by the Data Breaches and the public dissemination of her private information. She has incurred costs for credit monitoring. She has also suffered emotional distress, including fear, embarrassment, humiliation, a sense of impending doom, a fear of being recognized, and associated physical symptoms such as insomnia, nausea and headaches. Jane Doe 16 lives in fear that her family or professional colleagues will find her information online, including private photos.

Plaintiffs and Class Members Suffer Damages

191. Defendants negligently, and unlawfully, (i) failed to reasonably secure their patients' information, allowing malicious actors to access, copy, publish and disseminate extremely sensitive patient information; (ii) failed to adequately notify their patients of the breach (but rather misled them); (iii) failed to mitigate the harm by refusing to take reasonable steps to contain the further dissemination of the highly sensitive information; and (iv) failed to prevent a further intrusion into Defendants'

computer systems, thus (v) ultimately allowing it to happen all over again. Notwithstanding that Defendants were on notice of the exact risks realized, they failed to secure his patients' data. This is egregious conduct evincing a willful disregard of Plaintiffs' and Class Members' rights and safety.

192. The Data Breaches resulted from Defendants' inadequate cybersecurity and affirmative acts, which exposed Class Plaintiffs' and Class Members' confidential information to unauthorized cybercriminals who exfiltrated it. To date, Defendants have not disclosed the full details of the Data Breaches nor the findings of any investigations.

193. The Data Breaches were directly caused by Defendants' failure to employ reasonable cybersecurity measures and protocols to protect patients' information. Specifically, Defendants stored confidential data on a network left vulnerable to infiltration, thus permitting the hacking to succeed. Moreover, Defendants stored extremely sensitive patient data – *i.e.*, nude and during-surgery photographs – on inadequately secured portions of their network accessible via the internet. Defendants were aware of the known, prevalent threat of cyberattacks, recognizing that lacking security measures would leave Class Plaintiffs' and Class Members' information in jeopardy.

194. The consequences of Defendants' brazen failure to protect patients' confidential data are severe and enduring. Once stolen, such data can be misused for years. According to the Department of Justice, victims of data breaches are statistically more likely to experience identity fraud.

195. Both federal and state law generally prohibit healthcare providers from disclosing patients' confidential medical information without prior authorization.

196. Beyond statutory obligations, Defendants owed Plaintiffs and Class Members a common law duty to protect their confidential information by exercising reasonable care in obtaining, securing, safeguarding, deleting, and protecting it from unauthorized access, misuse, or disclosure.

197. As a direct result of Defendants' reckless and negligent conduct, unauthorized parties accessed, acquired, and misused Class Plaintiffs' and Class Members' confidential information, invading their privacy, exposing them to an increased risk of identity theft, public disclosure, and fraud.

198. Identity theft has serious consequences. While some victims resolve issues quickly, others spend significant time and money repairing damage to their credit, financial standing, and personal reputation. Some victims may lose job opportunities, be denied loans, or even face wrongful criminal charges due to fraudulent use of their identities.

199. Other potential consequences include fraudulent loans, unauthorized medical services billed under victims' names, tax fraud, and credit card fraud. In this case, the potential consequences, which were known and foreseeable to Defendants, include public disclosure of patients' private medical information and images.

200. Class Plaintiffs' and Class Members' confidential information has inherent value. Due to the breach, its value has diminished, while Defendants unjustly benefitted from failing to disclose their inadequate security measures.

201. Defendants had ample resources to prevent the breach but deliberately failed to implement adequate security measures, despite their legal obligations to protect patient data. Had Defendants implemented industry-recommended security measures, the breach and subsequent theft of Class Plaintiffs' and Class Members' confidential information could have been prevented.

202. Stolen confidential information can be exploited alone or combined with other publicly available data to commit additional fraud and wrongdoing. Hackers use such data for spear-phishing schemes, impersonating legitimate institutions to deceive victims into revealing even more sensitive information.

203. Additionally, the stolen information includes highly sensitive and humiliating videos and photographs of Class Plaintiffs and Class Members nude, partially clothed, under anesthesia, and undergoing surgery. The release and

threatened release of this data has caused and will continue to cause severe emotional distress to Class Plaintiffs and Class Members, compounding the harm.

204. Due to Defendants' wrongful actions and omissions, Plaintiffs and Class Members face ongoing risks, including:

a. The incessant threat of dissemination of private information including PII and PHI, medical diagnosis, extremely sensitive videos and images.

b. Fraudulent use of their confidential information;

c. Financial losses from identity theft;

d. Emotional distress and anxiety;

e. Future costs related to fraud prevention and monitoring.

205. Class Plaintiffs and Class Members have an undeniable interest in ensuring their confidential information remains secure and is not subject to further unauthorized access or misuse.

206. Defendants disregarded Class Plaintiffs' and Class Members' rights by willfully, recklessly, or negligently failing to protect their data systems; failing to disclose their inadequate computer systems and security practices; failing to take reasonable steps to prevent the Data Breaches; failing to monitor and detect the Data Breaches promptly; and failing to provide accurate and timely notice regarding the Data Breaches.

207. Because Defendants did not implement or adhere to reasonable data security protocols, Class Plaintiffs' and Class Members' PII and PHI was obtained by bad actors. Plaintiffs and Class Members have sustained or face a substantial risk of identity theft and fraud, forcing them to invest significant time and money to safeguard against further harm. They remain indefinitely vulnerable to heightened risk of identity theft and fraud.

208. Additionally, this is class is mainly comprised of vulnerable women particularly suspectable to humiliation on the basis of their appearance. Many victims

here suffer from a disfiguring conditions and have endured a lifetime of stares, glares, taunts and hurtful comments. Particularly distressing is the fact that nude photos and videos of class members' bodies (including some while under anesthesia) linked with their names, faces, and other identifying information, have been published not only on the dark web, but also on the public internet.

CLASS ACTION ALLEGATIONS

209. Class Plaintiffs bring this action as a class action pursuant to Federal Rule of Civil Procedure 23 on behalf of themselves and all other similarly situated persons in the following class:

All persons residing in the United States whose personal and medical information was compromised as a result of the Data Breaches (the "Class"). The Class excludes (a) Defendants and their relatives, employees, agents, attorneys, insurers, and representatives; (b) the Court and its staff; and (c) any persons who give notice that they wish to be excluded from the class pursuant to procedures to be specified by the Court.

210. Plaintiffs reserve the right to amend this Class and to add subclasses.

211. The Court should permit this action to be maintained as a class action pursuant to Federal Rule of Civil Procedure 23, because each of the requirements for class treatment is satisfied.

212. **Numerosity:** The Class is so numerous that the individual joinder of all members is impracticable. Plaintiffs are informed and believe that there are many hundreds if not thousands of total class members, and the class members are geographically dispersed.

213. **Typicality**. Class Plaintiffs' claims are typical of those of other class members. Each of the Class Plaintiffs had their sensitive Personal and Medical Information accessed and exfiltrated during the cybersecurity attacks described above.

214. **Commonality**. The claims of Class Members raise many common legal and factual issues, which predominate over any individualized issues, including,

without limitation, the following:

a. Whether Class Members' Personal and Medical Information stored on Defendants' system constituted protected personal identifying information and/or protected health information under state and federal law;

b. Whether Defendants acted negligently in connection with the monitoring and/or protecting of Class Plaintiffs' and Class Members' Personal and Medical Information

c. Whether and when Defendants actually learned of the First Hack and Second Hack and whether their response was adequate under law;

d. Whether Defendants were required under California and/or federal law to promptly notify affected patients of the data breaches;

e. Whether Defendants did promptly notify patients of the Data Breaches;

f. Whether Defendants owed a duty to the Class to exercise due care in collecting, obtaining, storing and/or safeguarding their Personal and Medical Information;

g. Whether Defendants breached that duty;

h. Whether Defendants implemented and maintained reasonable security procedures and practices appropriate to the nature of the risk of storing Class Plaintiffs' and Class Members' Personal and Medical Information;

i. Whether Defendants knew or should have known that they did not employ reasonable measures to keep Class Plaintiffs' and Class Members' Personal and Medical Information secure and prevent loss or misuse of that information;

j. Whether Defendants adequately addressed and fixed the vulnerabilities which permitted the Data Breaches to occur;

k. Whether Defendants caused Class Plaintiffs and Class Members damages through their negligent conduct and violation of statute;

l. Whether Defendants violated the California Unfair Competition

Law (Business & Professions Code § 17200, et seq.);

m. Whether Defendants violated the Confidentiality of Medical Information Act (Cal. Civ. Code § 56, et seq.); and

n. Whether Class members are entitled to actual damages, credit monitoring or other injunctive relief, and/or punitive damages as a result of Defendants' wrongful conduct.

215. **Adequacy**: Class Plaintiffs are adequate representatives of the Class. Class Plaintiffs are aware of their fiduciary obligations to Class Members, will fairly and adequately protect those interests, and have no disabling conflicts that would be antagonistic to those of Class Members. Class Plaintiffs have retained competent counsel, experienced in consumer class actions and other complex litigation.

216. **Superiority and Manageability**: Class litigation is an appropriate method for fair and efficient adjudication of the claims involved. Class treatment is superior to all other available methods for the fair and efficient adjudication of the controversy alleged herein in view of the large number of victims. It will permit a large number of Class Members to prosecute their common claims in a single forum simultaneously, efficiently, and without the unnecessary duplication of evidence, effort, and expense that hundreds of individual actions would require.

217. The nature of this action and the nature of laws available to Class Plaintiffs and the Class make the use of the class action device a particularly efficient and appropriate procedure to afford relief for the wrongs alleged. Absent class proceedings, Defendants would necessarily gain an unconscionable advantage since Defendants would be able to exploit and overwhelm the limited resources of each individual Class Member with superior financial and legal resources; the costs of individual suits could unreasonably consume the amounts that would be recovered; proof of a common course of conduct to which Plaintiffs were exposed is representative of that experienced by the Class and will establish the right of each Class Member to recover on the cause of action alleged; and individual actions would

create a risk of inconsistent results and would be unnecessary and duplicative.

218. Defendants are located and headquartered in California, are licensed n California, all plaintiffs were treated in California, on information and belief, all managerial decisions are made in California, and all the omissions and affirmative acts complained of herein occurred within California. Thus, application of California law is appropriate.

219. The litigation of the claims brought herein is manageable. Defendants' uniform conduct, the consistent provisions of the relevant laws, and the ascertainable identities of Class members demonstrates that there would be no significant manageability problems with prosecuting this lawsuit as a class action.

220. Adequate notice can be given to Class members directly using information maintained in Defendants' records.

221. Unless a Class-wide injunction is issued, Class Plaintiffs and Class Members remain at risk that Defendants will continue to fail to properly secure their confidential information, resulting in another data breach, continue to refuse to provide proper notification to Class Members regarding the Data Breaches, and continue to act unlawfully as set forth in this Complaint.

222. Defendants have acted or refused to act on grounds generally applicable to the Class and, accordingly, final injunctive or corresponding declaratory relief with regard to the Class members as a whole is appropriate under Rule 23(b)(2) of the Federal Rules of Civil Procedure.

FIRST CLAIM

VIOLATION OF THE CMIA

[Cal. Civ. Code § 56, *et seq.*]

(On Behalf of Plaintiffs and the Class)

223. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

224. At all relevant times, Defendants were providers of healthcare within the

meaning of California Civil Code § 56.06(a) and maintain medical information as defined by California Civil Code § 56.05.

225. Plaintiffs and Class Members are patients of Defendants, as defined in California Civil Code § 56.05(k).

226. Plaintiffs and Class Members provided their personal medical information to Defendants.

227. At all relevant times, Defendants collected, stored, managed, and transmitted Plaintiffs' and Class Members' personal medical information.

228. As a provider of health care, Defendants are required by the CMIA to ensure that medical information regarding patients is not disclosed, disseminated, or released without patients' authorization, and to protect and preserve the confidentiality of the medical information regarding a patient, under California Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, 56.36, and 56.101.

229. As a provider of health care, Defendants are required by the CMIA not to disclose medical information regarding a patient without first obtaining an authorization under California Civil Code §§ 56.06, 56.10, 56.13, 56.20, 56.245, 56.26, 56.35, and 56.104.

230. As a provider of health care, Defendants are required by the CMIA to create, maintain, preserve, and store medical records in a manner that preserves the confidentiality of the information contained therein under California Civil Code §§ 56.06 and 56.101(a).

231. As a provider of health care, Defendants are required by the CMIA to protect and preserve confidentiality of electronic medical information of Plaintiffs and the Class in its possession under California Civil Code §§ 56.06 and 56.101(b)(1)(A).

232. As a provider of healthcare, Defendants are required by the CMIA to take appropriate preventive actions to protect confidential information or records against release consistent with Defendants' obligations under California Civil Code § 56.36(2)(E).

233. As a result of the Data Breaches, Defendants have misused, disclosed, and/or allowed third parties to access, misuse, disclose, and view Plaintiffs' and Class Members' personal medical information without their written authorization compliant with the provisions of CMIA.

234. The bad actors who committed the Data Breaches obtained Plaintiffs' and Class Members' personal medical information, viewed it, and now have it available to sell or otherwise disclose to other bad actors for further misuse. They have already disclosed certain of that information both on the dark web and publicly.

235. Defendants' misuse and/or disclosure of medical information regarding Plaintiffs and Class members constitutes a violation of California Civil Code §§ 56.10, 56.11, 56.13, and 56.26.

236. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care, Plaintiffs' and Class Members' personal medical information was disclosed without written authorization.

237. By disclosing Plaintiffs' and Class Members' confidential information without their written authorization, Defendants violated California Civil Code § 56, *et seq*., and their legal duty to protect the confidentiality of such information.

238. Defendants also violated Sections 56.06 and 56.101 of the California Civil Code, which prohibit the negligent creation, maintenance, preservation, storage, abandonment, destruction, or disposal of confidential personal medical information.

239. As a direct and proximate result of Defendants' wrongful actions, inaction, omissions, and want of ordinary care that caused the Data Breach, Plaintiffs' and Class members' personal medical information was viewed by, released to, and disclosed to third parties without Plaintiffs' and Class members' written authorization.

240. Defendants' negligent and reckless failure to maintain, preserve, store, abandon, destroy, and/or dispose of Plaintiffs' and Class members' medical information in a manner that preserved the confidentiality of the information violated the CMIA, Cal. Civ. Code §§ 56.06 and 56.101(a). Accordingly, Defendants' systems

and protocols did not protect and preserve the integrity of electronic medical information in violation of the CMIA, Cal. Civ. Code § 56.101.

241. As a direct and proximate result of Defendants' and/or their employees' above-described conduct in violation of the CMIA, Plaintiffs and Class Members were injured and have suffered damages, as described above, from Defendants' illegal disclosure and/or negligent release of their medical information in violation of California Civil Code §§ 56.10 and 56.101.

242. Plaintiffs and Class members are therefore entitled to statutory damages of one thousand dollars ($1,000) for each violation under California Civil Code § 56.36(b)(1); the amount of actual damages, if any, for each violation under California Civil Code § 56.36(b)(2); injunctive relief; and attorneys' fees, expenses, and costs.

SECOND CLAIM

NEGLIGENCE

(On Behalf of Plaintiffs and the Class)

243. Plaintiffs restate and reallege all of the foregoing Paragraphs as if fully set forth herein.

Negligence

244. As a condition of receiving services, Plaintiffs and Class Members were obligated to provide Defendants directly, or through affiliates, with their confidential information.

245. Plaintiffs and Class Members entrusted their confidential information to Defendants with the understanding that Defendants would safeguard their information.

246. Defendants had full knowledge of the sensitivity of the confidential information and the types of harm that Plaintiffs and Class Members could and would suffer if the confidential information were wrongfully disclosed.

247. Defendants had a duty to exercise reasonable care in safeguarding, securing, and protecting such information from being compromised, lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes, among other

things, designing, maintaining, implementing, and testing security protocols to ensure that confidential information in their possession was adequately secured and protected, and that employees and vendors tasked with maintaining such information were adequately trained on relevant cybersecurity measures.

248. Plaintiffs and Class Members were the foreseeable and probable victims of any inadequate security practices and procedures. Defendants knew or should have known of the inherent risks in collecting and storing the confidential medical information of Plaintiffs and Class Members, the critical importance of providing adequate security for that information, the ongoing cyber threats and malicious actions being perpetrated against others in the medical field, and that their training, education, and IT security protocols were insufficient to secure the confidential information of Plaintiffs and Class Members.

249. Defendants' own conduct created a foreseeable risk of harm to Plaintiffs and Class Members. Defendants' misconduct included, but was not limited to, failing to take reasonably necessary steps to prevent the Data Breaches as set forth herein. Defendants' misconduct also included their decision not to comply with HIPAA and industry standards for the safekeeping and authorized disclosure of patient confidential information of Plaintiffs and Class Members.

250. Plaintiffs and Class Members had no ability to protect their Confidential Information that was in Defendants' possession.

251. Defendants were in a position to protect against the harm suffered by Plaintiffs and Class Members as a result of the Data Breach.

252. Defendants have at least partially admitted that Plaintiffs' and Class members' confidential information was wrongfully disclosed to unauthorized third persons as a result of the Data Breaches.

253. Through their actions and omissions, Defendants unlawfully breached their duty to Plaintiffs and Class Members by failing to exercise reasonable care in protecting and safeguarding Plaintiffs' and Class Members' confidential information

while it was within Defendants' possession or control.

254. Defendants improperly and inadequately safeguarded Plaintiffs' and Class Members' confidential information in deviation of standard industry rules, regulations, and practices at the time of the Data Breach.

255. Through their actions and omissions, Defendants unlawfully breached their duty to Plaintiffs and Class Members by failing to have appropriate procedures in place to detect and prevent dissemination of Plaintiffs' and Class Members' confidential information.

256. Through their actions and omissions, Defendants unlawfully breached their duty to adequately disclose to Plaintiffs and Class members the existence and scope of the Data Breaches.

257. Through their actions and omissions, Defendants failed to take reasonable steps to mitigate harm caused by their negligence including attempting to contain the further dissemination of private information.

258. But for Defendants' negligent breach of duties owed to Plaintiffs and Class Members, Plaintiffs' and Class Members' confidential information would not have been compromised and/or misused by unauthorized third parties to engage in fraudulent activity and public disclosure that further harmed Plaintiffs and Class Members.

259. There is a temporal and close causal connection between Defendants' failure to implement security measures to protect the confidential information and the harm suffered, or risk of imminent harm suffered, by Plaintiffs and the Class.

260. As a result of Defendants' negligence, unauthorized parties acquired Plaintiffs' and Class Members confidential information and used that information to harm Plaintiffs and Class Members as described above.

261. As a further result of Defendants' negligence, Plaintiffs and Class Members have suffered and will continue to suffer damages and injury including, but not limited to:

a. Severe emotional distress due to humiliation, shock, worry and anxiety over the incessant threat of publication, and actual publication, of confidential information including humiliating photos and videos of nude bodies and sensitive medical procedures along with identifying information, as well as identity theft;

b. actual identity theft;

c. an increased risk of identity theft, fraud, and/or misuse of their confidential information;

d. the loss of control over how their confidential information is used;

e. the compromise, publication, and/or theft of their information;

f. out-of-pocket expenses associated with the prevention, detection, and recovery from identity theft, and/or unauthorized use of their confidential information, and the value of their time in seeking to mitigate damages;

g. diminished value of the confidential information;

h. lost opportunity costs associated with efforts expended and the loss of productivity addressing and attempting to mitigate the actual and future consequences of the Data Breaches, including but not limited to efforts spent researching how to prevent, detect, contest, and recover from data breaches and identity theft;

i. the continued risk to their confidential information, which remains in Defendants' possession and is subject to further unauthorized disclosures as long as Defendants fail to undertake appropriate and adequate measures to protect confidential information in their continued possession; and

j. future costs in terms of time, effort, and money that will be expended to prevent, detect, contest, and repair the impact of the confidential information compromised as a result of the Data Breach for the remainder of the lives of Plaintiffs and Class Members.

Negligence Per Se

262. Violations of statutes that establish a duty to take precautions to protect a

particular class of persons from a particular injury or type of injury may constitute negligence *per se*. In addition to the statutes previously set forth, specific statutes governed the handling of Plaintiffs' and Class Members' sensitive information.

263. Section 5 of the FTC Act prohibits "unfair ... practices in or affecting commerce," including, as interpreted and enforced by the FTC, the unfair act or practice by businesses, such as Defendants, of failing to use reasonable measures to protect confidential information. The FTC publications and orders described above also form part of the basis of Defendants' duty in this regard.

264. Defendants violated Section 5 of the FTC Act by failing to use reasonable measures to protect Plaintiffs' and Class Members' confidential information and not complying with applicable industry standards, as described in detail herein. Defendants' conduct was particularly unreasonable given the nature and amount of confidential information they obtained and stored, and the foreseeable consequences of a data breach including, specifically, the damages that would result to Plaintiffs and Class Members.

265. Defendants' violation of Section 5 of the FTC Act constitutes negligence per se.

266. Plaintiffs and Class members are within the class of persons that the FTC Act was intended to protect.

267. The harm that occurred as a result of the Data Breaches is the type of harm the FTC Act was intended to guard against. The FTC has pursued enforcement actions against businesses which, as a result of their failure to employ reasonable data security measures and avoid unfair and deceptive practices, caused the same harm as that suffered by Plaintiffs and Class Members.

268. Defendants' violation of HIPAA also independently constitutes negligence per se.

269. HIPAA privacy laws were enacted with the objective of protecting the confidentiality of patients' healthcare information and setting forth the conditions

under which such information can be used, and to whom it can be disclosed. These privacy laws apply not only to healthcare providers and the organizations they work for, but to any entity that may have access to healthcare information about a patient, where exposure of such information could present a risk of harm to the patient's finances or reputation.

270. Plaintiffs and Class Members are within the class of persons that HIPAA privacy laws were intended to protect.

271. The harm that occurred as a result of the Data Breaches is the type of harm HIPAA privacy laws were intended to guard against.

272. As a direct and proximate result of Defendants' negligence *per se*, Plaintiffs and the Class have suffered, and continue to suffer, injuries and damages arising from the Data Breach including, but not limited to, an increased risk of identity theft, fraud, and/or misuse of their confidential information, damages from lost time and effort to mitigate the actual and potential impact of the Data Breaches on their lives, *e.g.*, by placing "freezes" and "alerts" with credit reporting agencies, contacting their financial institutions, closing or modifying financial and medical accounts, closely reviewing and monitoring their credit reports and various accounts for unauthorized activity, and filing police reports. Plaintiffs and Class Members have also suffered severe emotional distress as alleged above.

273. Plaintiffs and Class Members have also suffered damages, which may take months if not years to discover and detect.

274. Defendants' conduct, as alleged herein, was willful, fraudulent, and malicious. Defendants deliberately disregarded the need to safeguard Plaintiffs' and Class Members' confidential information and were willfully indifferent to the risk to Plaintiffs and Class Members of wrongful access to and disclosure of their confidential information. In addition, Defendants misled Plaintiffs and Class Members as to the facts surrounding the Data Breaches, including the nature and scope of the breaches, and the reasons the breaches occurred.

//

THIRD CLAIM

VIOLATION OF THE CALIFORNIA UNFAIR COMPETITION LAW

CAL. BUS. & PROF. CODE §§ 17200, ET SEQ. ("UCL")

(On Behalf of Plaintiffs and the Class)

275. Plaintiffs restate and reallege all of the foregoing Paragraphs as if fully set forth herein.

276. The California Unfair Competition Law, Cal. Bus. & Prof. Code, § 17200, *et seq.* ("UCL"), prohibits any "unlawful," "fraudulent," or "unfair" business act or practice and any false or misleading advertising, as defined by the UCL and relevant case law.

277. By reason of Defendants' above-described wrongful actions, inaction, and omissions, the resulting Data Breaches, and the unauthorized disclosure of Plaintiffs and Class Members' confidential information, Defendants engaged in unlawful, unfair, and fraudulent practices within the meaning of the UCL.

278. In the course of conducting their business, Defendants committed "unlawful" business practices by, *inter alia*, knowingly failing to design, adopt, implement, control, direct, oversee, manage, monitor, and audit appropriate data security processes, controls, policies, procedures, protocols, and software and hardware systems to safeguard and protect Plaintiffs' and Class Members' PII/PHI, and by violating the statutory and common law alleged herein, including, inter alia, California's CMIA (Civ. Code §§ 56.10(a), (e); 56.101(a), 56.101(b)(1)(A); 56.36), the California Consumer Privacy Act of 2018 ("CCPA") (Cal. Civ. Code § 1798.150(a)(1)), the Health Insurance Portability and Accountability Act of 1996 (42 U.S.C. § 1302d; 45 C.F.R. §§ 164.306(a), (d), (e); 164.308(a); 164.312(a), (d), (e); 164.316(a), (b)), California Civil Code § 1798.81.5, and Article I, Section 1 of the California Constitution (constitutional right to privacy).

279. Defendants also violated the UCL by failing to adequately and timely

notify Plaintiffs and Class members pursuant to California Civil Code § 1798.82(a) regarding the unauthorized access and disclosure of their PII/PHI. Had Plaintiffs and Class Members been adequately and timely notified in an appropriate fashion, they could have taken precautions to safeguard and protect their PII/PHI and identities.

280. Defendants' above-described wrongful actions, inaction, and omissions, the resulting Data Breaches, and the unauthorized release and disclosure of Plaintiffs' and Class Members' confidential information also constitute "unfair" business acts and practices within the meaning of the UCL in that Defendants' conduct was substantially injurious to Plaintiffs and Class Members, offensive to public policy, immoral, unethical, oppressive, and unscrupulous, and the gravity of Defendants' conduct outweighs any alleged benefits attributable to such conduct. Said acts, omissions and inaction violated strong public policies embodied in the California Constitution, the CMIA, the CCPA, and HIPAA.

281. In addition, Defendants engaged in unlawful acts and practices by failing to disclose the Data Breaches in a timely and accurate manner, contrary to the duties imposed by Cal. Health & Safety Code § 1280.15(b)(2).

282. Plaintiffs and Class members suffered (and continue to suffer) injury in fact, invasion of privacy, and lost money or property as a direct and proximate result of Defendants' above-described wrongful actions, inaction, and omissions including, inter alia, the unauthorized release and disclosure of their confidential information. Plaintiffs lost money or property by paying for a certain level of security for their PII/PHI but receiving a lower level and paying more for Defendants' products and services than they otherwise would have paid had they known Defendants were not providing the reasonable security represented in Defendants' stated privacy policies and as required by law. Defendants' security practices have economic value in that reasonable security practices reduce the risk of theft of PII/PHI collected, maintained, and stored by Defendants.

283. Defendants knew or should have known that their computer systems and

data security practices were inadequate to safeguard Plaintiffs' and Class Members' confidential information and that the risk of a data breach or theft was highly likely. Defendants' actions in engaging in the above-named unlawful practices and acts were negligent, knowing, and willful, and/or wanton and reckless with respect to the rights of Plaintiffs and Class members.

284. Plaintiffs seek prospective injunctive relief, including improvements to Defendants' data security systems and practices, in order to ensure that such security is reasonably sufficient to safeguard patients' private information that remains in Defendants' custody.

285. Unless such class-wide injunctive relief is issued, Defendants will continue to engage in the above-described wrongful conduct, more data breaches will occur, Plaintiffs and Class Members will remain at risk, and there is no other adequate remedy at law that would ensure Plaintiffs (and other consumers) can rely on Defendants' representations regarding data security in the future.

286. Furthermore, in the alternative to legal remedies sought herein Plaintiffs and the class further seek restitution of money or property that Defendants have acquired by means of Defendants' unlawful and unfair business practices; restitutionary disgorgement of all profits accruing to Defendants because of Defendants' unlawful and unfair business practices; declaratory relief; attorneys' fees and costs (pursuant to Cal. Code Civ. Proc. § 1021.5); and injunctive or other equitable relief.

FOURTH CLAIM

INVASION OF PRIVACY

(On Behalf of Plaintiffs and the Class)

287. Plaintiffs restate and reallege all of the foregoing Paragraphs as if fully set forth herein.

288. California established the right to privacy in Article 1, Section 1 of the California Constitution.

289. Plaintiffs and Class Members had a legitimate and reasonable expectation of privacy with respect to their confidential information and were entitled to protection of this information against disclosure to unauthorized third parties.

290. Defendants owed a duty to patients, including Plaintiffs and Class Members, to keep their confidential information confidential.

291. The unauthorized access to and release of confidential information, especially personal health information, photographs, and video, is highly offensive to a reasonable person.

292. The intrusion was into a place or thing, which was private and entitled to be private. Plaintiffs and Class Members disclosed their confidential information to Defendants as part of their use of Defendants' medical services, with the intention and reasonable understanding that the confidential information would be kept confidential and protected from unauthorized access and disclosure. Plaintiffs and Class Members were reasonable in their belief that such information would be kept private and would not be disclosed without their authorization.

293. The Data Breaches constitute an intentional interference with Plaintiffs' and Class Members' interest in solitude or seclusion, either as to their persons or as to their private affairs or concerns, of a kind that would be highly offensive to a reasonable person.

294. Defendants acted with a knowing state of mind when they permitted the Data Breaches because they knew their information security practices were inadequate and would likely result in a data breach such as the one that harmed Plaintiffs and Class Members.

295. Acting with knowledge, Defendants had notice that their inadequate cybersecurity practices would cause injury to Plaintiffs and Class Members.

296. As a proximate result of Defendants' acts and omissions, Plaintiffs' and Class Members' confidential information was disclosed to and used by third parties without authorization in the manner described above, causing Plaintiffs and Class

Members to suffer damages.

297. Unless and until enjoined and restrained by order of this Court, Defendants' wrongful conduct will continue to cause great and irreparable injury to Plaintiffs and Class Members in that the confidential information maintained by Defendants can be viewed, distributed, and used by unauthorized persons.

298. Plaintiffs and Class members have no adequate remedy at law for the injuries because a judgment for monetary damages will not end the invasion of privacy for Plaintiffs and Class members.

FIFTH CLAIM

VIOLATION OF CAL. CIV. CODE § 1798.80 ET SEQ.

(On Behalf of Plaintiffs and the Class)

299. Plaintiffs restate and reallege all of the foregoing paragraphs as if fully set forth herein.

300. Section 1798.2 of the California Civil Code requires any "person or business that conducts business in California, and that owns or licenses computerized data that includes personal information" to "disclose any breach of the security of the system following discovery or notification of the breach in the security of the data to any resident of California whose unencrypted personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Under section 1798.82, the disclosure "shall be made in the most expedient time possible and without unreasonable delay ...."

301. The CCRA further provides: "Any person or business that maintains computerized data that includes personal information that the person or business does not own shall notify the owner or licensee of the information of any breach of the security of the data immediately following discovery, if the personal information was, or is reasonably believed to have been, acquired by an unauthorized person." Cal. Civ. Code § 1798.82(b).

302. Any person or business that is required to issue a security breach

notification under the CCRA shall be written in plain language and contain the following information:

a. The name and contact information of the reporting person or business subject to this section;

b. A list of the types of personal information that were or are reasonably believed to have been the subject of a breach;

c. If the information is possible to determine at the time the notice is provided, then any of the following:

i. The date of the breach;

ii. The estimated date of the breach; or

iii. The date range within which the breach occurred.

iv. The notification shall also include the date of the notice. Whether notification was delayed as a result of a law enforcement investigation, if that information is possible to determine at the time the notice is provided;

v. A general description of the breach incident, if that information is possible to determine at the time the notice is provided; and

vi. The toll-free telephone numbers and addresses of the major credit reporting agencies if the breach exposed a Social Security number or a driver's license or California identification card number.

303. The Data Breaches described herein constituted a "breach of the security system" of Defendants.

304. As alleged above, Defendants unreasonably delayed informing Plaintiffs and Class Members about the Data Breaches, affecting their Personal and Medical Information, after Defendants knew the Data Breaches had occurred.

305. Defendants failed to disclose to Plaintiffs and Class Members, without unreasonable delay and in the most expedient time possible, the breach of security of their unencrypted, or not properly and securely encrypted, Personal and Medical Information when Defendants knew or reasonably believed such information had been

compromised.

306. Defendants' ongoing business interests gave Defendants incentive to conceal the Data Breaches from the public to ensure continued revenue, which Defendants did for many months.

307. Upon information and belief, no law enforcement agency instructed Defendants that timely notification to Plaintiffs and Class members would impede its investigation.

308. As a result of Defendants' violation of California Civil Code § 1798.82, Plaintiffs and Class Members were deprived of prompt notice of the Data Breaches and were thus prevented from taking appropriate protective measures, such as securing identity theft protection or requesting a credit freeze. These measures could have prevented some of the damages suffered by Plaintiffs and Class Members because their stolen information would have had less value to identity thieves.

309. In addition, Defendants' failure to notify appropriate authorities also prevented public disclosure of the Data Breaches through government agencies and the news media. As a result many victims, who were entitled to and otherwise would have received notice that their data had been compromised, were deprived of notice.

310. As a result of Defendants' violation of California Civil Code § 1798.82, Plaintiffs and Class members suffered incrementally increased damages separate and distinct from those simply caused by the Data Breaches itself.

311. Plaintiffs and Class members seek all remedies available under California Civil Code § 1798.84, including, but not limited to, the damages suffered by Plaintiffs and Class Members as alleged above and equitable relief.

312. Because Defendants' violations were willful, intentional, and/or reckless, Plaintiffs seek civil penalties not to exceed $3,000 per violation or, in the alternative, $500 per violation pursuant to California Civil Code § 1798.84, as well as attorney's fees and costs.

//

PRAYER FOR RELIEF

WHEREFORE, Class Plaintiffs, on behalf of themselves and all members of the Class, pray for relief as follows:

A. An order certifying this action as a class action under Federal Rule of Civil Procedure 23, defining the Class and any subclasses requested herein, appointing the undersigned as Class Counsel, and finding that each of the named Plaintiffs is an appropriate representative of the certified Class;

B. Injunctive relief requiring Defendants to (1) adopt, implement, and maintain reasonable data security systems that maintain personally identifying information to comply with the applicable law and industry standards; (2) engage third-party auditors and internal personnel to determine the scope of the Data Breaches and the patients whose records were compromised; (3) conduct security testing and audits on Defendants' systems on a periodic basis to ensure compliance; (4) promptly correct any problems or issues detected by such audits and testing; (5) conduct periodic training to inform internal personnel how to prevent, identify and contain a breach, and how to appropriately respond; and (6) to provide accurate notice of the nature and scope of the Data Breaches, and the compromised data, to all affected patients.

C. An award of credit monitoring and identity theft protection services to Plaintiffs and all members of the Class;

D. Actual, compensatory, consequential, incidental, nominal, and statutory damages;

E. Restitution and restitutionary disgorgement;

F. Statutory damages and penalties, trebled, and/or punitive or exemplary damages, to the extent permitted by law, including, but not limited, to the following:

1. Damages not to exceed three thousand dollars ($3,000) per violation, attorney's fees not to exceed one thousand dollars ($1,000) per violation, and the costs of litigation under California Civil Code § 56.35;

2. Statutory damages of one thousand dollars ($1,000) for each violation under California Civil Code § 56.36(b)(1);

3. Actual damages suffered, according to proof, for each violation under California Civil Code § 56.36(b)(2);

4. Damages of $3,000 per violation of Civil Code section 1798.83 or, in the alternative, $500 per violation, pursuant to Civil Code §§ 1798.84(b);

G. Punitive damages pursuant to California Civil Code § 3294;

H. Nominal damages according to proof;

I. Attorney's fees pursuant to the common fund doctrine and as provided by law, including, without limitation, under California Civil Code §§ 56.35 and 1798.84, and California Code of Civil Procedure § 1021.5.

J. An award of costs of suit as provided by law;

K. Pre- and post-judgment interest as provided by law;

L. Such other and further relief as the Court may deem just and proper.

Dated: April 4, 2025

Respectfully submitted,
ROBINSON MARKEVITCH & PARKER LLP

By: /s/ Damion Robinson
Damion D. D. Robinson
David Markevitch
Jimmie Davis Parker

Attorneys for Class Plaintiffs and all others similarly situated

DEMAND FOR JURY TRIAL

Class Plaintiffs demand a trial by jury on all matters so triable.

Dated: April 4, 2025

Respectfully submitted,
ROBINSON MARKEVITCH & PARKER LLP

By: /s/ Damion Robinson
Damion D. D. Robinson
David Markevitch
Jimmie Davis Parker

Attorneys for Class Plaintiffs and all others similarly situated

PROOF OF SERVICE

I, the undersigned, certify that I have filed the foregoing document using the Court's CM/ECF platform. I am informed and believe that filing through the CM/ECF system will result in electronic notice to all parties who have signed up to receive electronic notice, including counsel for all parties who have appeared in the action.

I declare under penalty of perjury under the laws of the United States that the foregoing is true and correct.

Dated: April 4, 2025

Damion Robinson